Supliment al revistei „Impact strategic”

COLOCVIU STRATEGIC

UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I”

CENTRUL DE STUDII STRATEGICE DE APĂRARE ȘI SECURITATE

Nr. 7 (166) / 2019
Indexat în CEEOL

CREAREA UNEI ECHIPE DE INTERVENȚIE ÎN CAZ DE INCIDENTE DE SECURITATE INFORMATICĂ LA NIVELUL POLIȚIEI ROMÂNE

Ion PARASCHIVA

Setting up a Computer Emergency Response Team for the Romanian Police

Abstract: *By creating its own Computer Emergency Response Team, Romanian Police will be able to provide the exchange of information between the SISPOL users, other authorities and providers of cyber security equipment and solutions. It will also identify, analyse and classify cyber security incidents within SISPOL and provide IT consultancy from specialists of the Romanian Police and other actors involved in the security of SISPOL. In practice, Computer Security Incident Response Team will have the objective of combatting and countering cyber-space threats in order to improve SISPOL security, to prevent and to counteract IT security incidents and cyber-attacks.*

Keywords: *Cyber security, Computer Emergency Response Team (CERT), Computer Security Incident Response Team (CSIRT), Cyber security strategy, private cloud.*

Crearea unei echipe de intervenție în caz de incidente de securitate informatică la nivelul Poliției Române

Rezumat: *Prin crearea propriei structuri de tip CERT, Poliția Română va asigura schimbul de informații dintre utilizatorii Sistemului Informatic Sectorial al Poliției Române (SISPOL), celelalte autorități și furnizorii de echipamente hardware și software în domeniul securității cibernetice. De asemenea, va identifica, analiza și clasifica incidentele de securitate cibernetică din cadrul SISPOL și va asigura consultanță specialiștilor IT din cadrul Poliției Române și celorlalți actori implicați în asigurarea securității SISPOL. Practic, CSIRT va avea ca obiectiv combaterea și contracararea amenințărilor din spațiul cibernetic, în scopul îmbunătățirii securității SISPOL, prevenirii și contracarării incidentelor de securitate IT și atacurilor cibernetice.*

Cuvinte-cheie: *securitate cibernetică, Centrul de Răspuns la Incidente de Securitate Cibernetică (CERT), echipa de intervenție în caz de incidente de securitate informatică (CSIRT), strategie de securitate cibernetică, cloud privat.*

1. Serviciile CERT la nivel (inter)național

Odată cu adoptarea tehnologiei la scară largă s-a intensificat și numărul atacurilor cibernetice și astfel, statele au fost nevoite să-și dezvolte o serie de instituții care să răspundă la aceste noi tipuri de incidente informatice. Printre primii care au identificat această necesitate a fost Departamentul american al apărării, care a finanțat, începând cu anul 1984, cercetarea și dezvoltarea de instrumente de apărare împotriva amenințărilor cibernetice la Institutul de Inginerie Software[1].

Entitățile de tip CERT au în vedere, pe lângă prevenirea, detectarea și răspunsul la amenințările de securitate cu privire la sistemele informaționale, și asigurarea de informații legate de incidentele de securitate pentru utilizatorii sistemelor informaționale prin intermediul Internetului.

Termenul CERT/CSIRT provine din limba engleză (Computer Emergency Response Team / Computer Security Incident Response Team) și este tradus în limba română prin mai multe variante, „Echipa de răspuns la urgențe cibernetice”,

***Ion PARASCHIVA**, Șef Serviciu Administrare Sisteme Informatice la Direcția de Comunicații și Informatică a Inspectoratului General al Poliției Române, este doctorand în domeniul Ordine Publică și Siguranță Națională în cadrul Academiei de Poliție „Alexandru Ioan Cuza” din București, e-mail: ion@paraschiva.com.*

„Echipa de răspuns la incidente de securitate cibernetică” sau „Echipa de intervenție în caz de incidente de securitate informatică”[2].

În funcție de „organizațiile pe care le deservesc, de nivelul de autoritate sau de competențele pe care le dețin, echipele CERT se încadrează în una sau mai multe din următoarele categorii: național; guvernamental; academic; privat”[3].

La nivelul țării noastre există Centrul National de Răspuns la Incidente de Securitate Cibernetică (CERT-RO), ca structură independentă de expertiză și cercetare-dezvoltare în domeniul protecției infrastructurilor cibernetice, aflată în coordonarea Ministerului Comunicațiilor și Societății Informaționale[4].

Potrivit CERT-RO, „România are atât rol generator de incidente de securitate cibernetică, cât și rol de proxy (de tranzit) pentru atacatorii din afara spațiului național prin prisma utilizării unor sisteme informatice vulnerabile sau compromise, ce fac parte din spațiul cibernetic național”[5]. Statisticile din anul 2017[6] arată că „CERT-RO a colectat și procesat 138.217.026 de alerte de securitate cibernetică, în creștere cu 25% față de anul 2016 (110.194.890). Principalele cinci tipuri de amenințări cibernetice manifestate în perioada analizată au fost: malware; ransomware; botnets; DDoS; phishing”.

În sensul dezvoltării SISPOL către o infrastructură de *cloud privat*[7] și, nu în ultimul rând, ținând cont de natura informațiilor sensibile vehiculate în cadrul instituției, problema securității cibernetice trebuie tratată cu prioritate. În acest context, consider că un prim pas ar fi ca, Poliția Română, împreună cu CERT-RO, să dezvolte o strategie de securitate dedicată pentru instituția responsabilă de aplicarea legii în România. Această strategie trebuie să pună accent pe următoarele aspecte:

1. stabilirea viziunii și a scopului Poliției Române cu privire la dezvoltarea cloud-ului privat;
2. identificarea componentelor considerate critice în cadrul sistemului informatic sectorial al Poliției Române;
3. stabilirea unei baze de date cu privire la securitatea cibernetică în cloud-ul privat și urmărirea cu rigurozitate a implementării recomandărilor identificate;
4. identificarea unui echilibru între asigurarea securității informatice și oferirea a cât mai multor resurse polițiștilor din teren;
5. stabilirea unei strategii de răspuns la incidente;
6. realizarea exercițiilor de securitate cibernetică pentru a identifica modul de răspuns al Poliției Române la atacurile cibernetice și posibilitatea de a-l îmbunătății;
7. instruirea personalului cu privire la amenințările de securitate și a modalităților de a se proteja de acestea;
8. pregătirea continuă a specialiștilor responsabili de securitatea informatică din cadrul Poliției Române;
9. cooperarea internațională și adoptarea tehnicilor și strategiilor implementate cu succes în instituții similare ale altor state.

Prin dezvoltarea propriului CSIRT, specialiștii responsabili din cadrul Poliției Române vor acționa mult mai rapid în fața unor amenințări și incidente de securitate cibernetică.

2. Un model de CSIRT la nivelul Poliției Române

Unul din motivele fundamentale pentru care Poliția Română trebuie să-și creeze propria echipă de răspuns la incidentele legate de securitatea cibernetică este acela de a-și proteja întreaga infrastructură SISPOL. Este nevoie de specialiști în securitatea cibernetică care să gestioneze incidentele de securitate și să sprijine polițiștii în recuperarea datelor ca urmare a încălcărilor procedurilor de securitate. De asemenea, având propria echipă de răspuns la incidentele legate de securitatea cibernetică, Poliția Română ar reduce substanțial costurile legate de contractarea unor firme care, pe de o parte, să asigure securitatea sistemelor informatice pe care le deține și, pe de altă parte, să ofere consultanță în legătură cu vulnerabilitățile din echipamentele hardware și software utilizate.

CSIRT propus a fi dezvoltat în cadrul Poliției Române va avea o politică proprie pentru securitatea informațiilor, care, pe lângă faptul că descrie starea dorită a proceselor și procedurilor operaționale și administrative, trebuie să se alinieze cu legislația și standardele în vigoare. Echipa va furniza următoarele tipuri de servicii:

1. *Servicii de răspuns*: alerte și avertizări; gestionarea incidentelor; analiza incidentelor; asistență de răspuns la incidente; coordonarea răspunsului la incidente; răspunsul la incidente la fața locului; gestionarea vulnerabilității; analiza vulnerabilității; răspunsul la vulnerabilitate; coordonarea răspunsului la vulnerabilitate.
2. *Servicii în avans*: anunțuri; supravegherea tehnologiei; audituri sau evaluări de securitate; configurarea și întreținerea securității; dezvoltarea instrumentelor de securitate; servicii de detectare a intruziunii; diseminarea informațiilor de securitate.
3. *Gestionarea artefactelor*: analiza artefactelor; răspunsul la artefacte; coordonarea răspunsului la artefacte.
4. *Managementul de calitate a securității*: analiza riscurilor; continuitatea afacerilor și recuperarea în urma dezastrelor; consultanță de securitate; dezvoltarea gradului de cunoaștere; educația/ formarea; evaluarea sau certificarea produselor.

Activitatea CSIRT de la nivelul Poliției Române se va desfășura pe două componente:

1. *Componenta defensivă* care cuprinde activitatea de identificare, analizare, răspuns, investigare și monitorizare a incidentelor de securitate.

2. *Componenta ofensivă* care cuprinde activitatea de prevenire a incidentelor de securitate IT, prin utilizarea unor teste și acțiuni proactive specifice.

Echipa CSIRT va cuprinde specialiști IT din cadrul Poliției Române, specialiști care trebuie instruiți astfel încât să înțeleagă progresul tehnologic și modul în care infractorii cibernetici acționează, având în vedere că echipa are responsabilitatea de a implementa anumite tehnologii de securitate la nivelul SISPOL, precum soluții antivirus și firewall, și de a configura echipamentele hardware și aplicațiile software având în vedere practicile de securitate. Mandatul CSIRT va fi de a susține Poliția Română în protejarea împotriva incidentelor IT, coordonând și raportând incidentele de securitate cu care se confruntă această instituție. Printre atribuțiile echipei este și descoperirea vulnerabilităților („patch-urilor" de securitate").

În ceea ce privește personalul CSIRT[8] sugerez un număr maxim de 30 persoane (după cum se poate observa în figura nr. 1), care să facă parte din personalul CSIRT de la nivelul Poliției Române. Aceștia trebuie să îndeplinească următoarele atribuții/criterii:

1. *Director* - planificarea, dezvoltarea și implementarea strategiilor operaționale, a inițiativelor, politicilor și programelor CSIRT și, nu în ultimul rând, urmărește și evaluează îndeplinirea planului strategic al CSIRT.

2. *Director Adjunct* - planificarea, dezvoltarea și implementarea strategiilor operaționale, a inițiativelor, politicilor și programelor CSIRT și, nu în ultimul rând, urmărește și evaluează îndeplinirea planului strategic al CSIRT. El este cel care înlocuiește directorul, în cazul indisponibilității acestuia.

3. *Șef Serviciu* - planificarea, dezvoltarea și implementarea strategiilor operaționale la nivelul fiecărui serviciu, precum și monitorizarea și identificarea problemelor apărute pe linia lor de muncă. Tot ei sunt cei care coordonează activitatea specifică fiecărui serviciu.

4. *Analist securitate Internet*:

- testarea și analizarea codurilor malițioase, a software-lor vulnerabile, instrumentelor de actualizări de securitate;

- dezvoltarea sau asigurarea unei imagini globale a evoluției SISPOL și proceselor interne care să conducă la analize;

- analizarea și identificarea tendințelor în domeniul securității pe baza incidentelor, precum și analiza informațiilor publice și colaborarea cu alți experți în domeniul securității IT;

- elaborarea de documente care să descrie cele mai bune practici pentru SISPOL și pentru administratorii de rețea, managerii tehnici și alți tehnicieni;

- reprezentarea CSIRT la diverse forumuri tehnice și asigurarea de îndrumare tehnică pentru ceilalți membri ai echipei;

- participarea activă la elaborarea de planuri strategice și direcții de dezvoltare ale CSIRT;

- monitorizarea informațiilor de rutare și a serverelor cheie DNS și publicarea acestor informații;

- publicarea de lucrări și prezentări în colaborare cu părți interne și externe pe problematica securității rețelelor și Internetului.

5. *Specialist în domeniul vulnerabilităților IT*:

- cercetarea în detaliu a vulnerabilității software;

- corespondență cu furnizorii de software;

- crearea de specificații și dezvoltarea de instrumente și procese pentru îndeplinirea scopului echipei;

- coordonarea activităților de stabilire a direcțiilor de strategie în cercetarea vulnerabilității și identificarea și implementarea de noi abordări pentru analizarea și prevenirea vulnerabilităților de software.

6. *Specialist în dezvoltarea practicilor și instruire*:

- dezvoltarea și predarea practicilor de îmbunătățire a securității și crearea de programe de instruire în asigurarea și siguranța informațiilor pentru administratorii și managerii de sistem și rețea;

- lucrul cu clienții din diverse organizații, inclusiv agenții guvernamentale și alte instituții care se ocupă de infrastructuri critice.

7. *Analist statistic pentru securitatea rețelei*:

- dezvoltarea de instrumente de analiză;

- participarea la dezvoltarea unui program de analizare a datelor de securitate a rețelei.

8. *Administrator de sistem*:

- susținerea utilizatorilor și întreținerea software-ului și a echipamentelor din cadrul CSIRT;

- dezvoltarea unor servicii experimentale care să răspundă acestor necesități;

- planificarea achizițiilor de echipamente, a configurației și întreținerii echipamentelor, a instalării și scoaterea lor din uz.

9. *Specialist informare tehnică și relații publice*:

- să cunoască conceptele generale de IT și terminologia specifică în engleză și română;

- să aibă capacități de editare/manipulare și cunoștințe generale de „web design".

10. *Consultant securitate*:

- să aibă experiență ca administrator într-un sistem de tip Windows sau UNIX, în arhitectură de sistem, soluții totale de securitate și protocoale și aplicații de Internet;

- să aibă experiență în configurarea și implementarea de soluții tehnice de securitate (firewalls și sisteme de detectare a intruziunilor);

- să aibă capacități de interfață cu clienții, bune capacități de comunicare verbală și în scris, precum și capacități de management de proiect, cu-

noștințe de protocoale și aplicații comune de Internet;

- să dețină certificate de tipul MSCE, CCNA, CISSP, CISM, CISA.

11. *Inginer de securitate*:

- să aibă capacitatea de a citi și înțelege cod de asamblare x86 și cunoștințe de rețele CP/IP, inclusiv informații privind protocoalele TCP/IP;

- să aibă experiență în programare C/C++ pe platforme MS Windows și/sau Linux;

- să aibă cunoștințe de lucru în „shell scripting”, programare PERL și/sau Python.

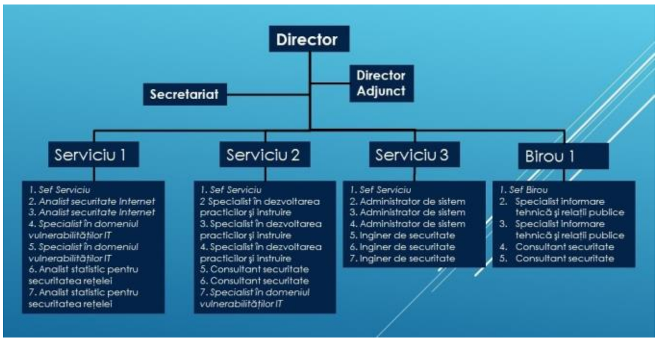


Figura nr. 1 – Propunere de organigramă pentru CSIRT

Echipa de răspuns la incidentele legate de securitatea cibernetică creată la nivelul Poliției Române va avea următoarele atribuții:

1. va asigura suportul tehnic administratorilor SISPOL pentru aplicarea celor mai bune practici ale securității;
2. va detecta vulnerabilitățile și intruziunile în infrastructura SISPOL;
3. va monitoriza incidentele de securitate a rețelelor și sistemelor informatice de la nivelul Poliției Române;
4. va emite avertizări timpurii, alerte și anunțuri și va avea o reacție oportună la apariția incidentelor de securitate IT;
5. va stabili impactul la nivelul SISPOL al incidentelor și va informa factorii de decizie din cadrul Poliției Române;
6. va asigura răspunsul la incidente:
7. va elabora analize de risc, de incident și sensibilizare;
8. va preveni atacurile externe asupra infrastructurii SISPOL;
9. va realiza schimbul de informații cu echipa CSIRT națională din cadrul CERT-RO prin intermediul platformei de management a incidentelor.

Mergând chiar mai departe, echipa CSIRT va elabora, pentru SISPOL, planul de recuperare în caz de dezastre cu impact major și va planifica activitățile astfel încât să se asigure funcționarea acestora în cazul unor incidente de tipul atacului „Ransomware WannaCry”[9].

Echipa CSIRT trebuie să dețină informații cu privire la întreaga arhitectură a SISPOL și nu în ultimul rând, să cunoască activitatea specifică a Poliției Române. Prin crearea propriului CSIRT, structura de poliție ar înregistra următoarele beneficii:

1. Existența unei coordonări centralizate pentru problemele de securitate informatică în interiorul Inspectoratului General al Poliției Române.
2. Răspuns centralizat la incidentele de securitate cibernetică.
3. Existența la îndemână a expertizei care să sprijine specialiștii IT din cadrul Poliției Române să readucă sistemul la starea normală de funcționare după apariția unor incidente de securitate cibernetică.
4. Soluționarea problemelor legale și păstrarea probelor în cazul unui proces civil.
5. Urmărirea dezvoltărilor din domeniul securității.
6. Stimularea cooperării cu beneficiarii în domeniul securității informatice (sensibilizare).

3. Legătura dintre CSIRT și SISPOL

Ținând cont de atacurile informatice din ultimul timp, componenta de securitate IT de la nivelul Poliției Române devine un punct critic în realizarea și menținerea unui sistem informatic sigur și funcțional. Astfel, un antivirus actualizat și un firewall activat nu mai reprezintă metode suficiente de protecție la nivelul SISPOL.

Deși, pe termen scurt, securitatea SISPOL presupune îndeplinirea atributelor de integritate, disponibilitate și confidențialitate, pe termen lung, protecția valorilor Poliției Române și asigurarea continuității serviciilor impune o serie de măsuri:

1. *Preventive*: informarea și conștientizarea specialiștilor IT din cadrul Poliției Române, crearea unei culturi organizaționale privind securitatea, pentru o mai ușoară identificare și conștientizare a riscurilor și amenințărilor și, nu în ultimul rând, instruirea utilizatorilor SISPOL.
2. *Protective*: măsuri tehnice de protecție, utilizarea de echipamente și dispozitive securizate și planuri de recuperare în caz de dezastru.
3. *De revizuire și perfecționare continuă*: controale periodice, urmărirea progreselor tehnologice și adaptarea la noile tehnologii.

Este de necontestat importanța și rolul pe care îl are partea tehnică într-un sistem de securitate protectiv/reactiv, dar mecanismele tehnice de apărare nu fac față prejudiciilor provocate de incidentele de securitate cibernetică dacă nu sunt sprijinite de „resursa umană”, care controlează în final echipamentele.

Strategia de securitate[10], care trebuie dezvoltată împreună cu CERT-RO, are ca țintă o serie de măsuri și acțiuni legate de securitatea informatică specifică cloud-ului privat, ca și componentă informatică. Însă, având în vedere componentele cloud-ului privat, consider că este necesară stabilirea unor strategii de securitate dedicate pentru fieca-

re componentă. Această situație presupune ca, Poliția Română să dețină o structură proprie de răspuns la incidentele informatice, echipă formată din specialiști pe securitatea:

1. rețelei de comunicații;
2. dispozitivelor de procesare și stocare;
3. sistemelor de operare;
4. sistemelor de backup;
5. dispozitivelor mobile;
6. aplicațiilor;
7. bazelor de date;
8. fizică.

O structură astfel formată ar permite Poliției Române să acopere securitatea tuturor componentelor cloud-ului privat și să răspundă în acest fel necesităților impuse de evoluția spre o astfel de infrastructură.

De asemenea, pentru a trata cât mai eficient situațiile de criză generate de amenințările cibernetice este necesară realizarea unei camere de comandă, care să cuprindă specialiștii de securitate ai tuturor componentelor cloud-ului privat. Printre beneficiile generate de această cameră de comandă, menționăm:

1. eficiență crescută în colaborarea între membrii echipei de răspuns la incident;
2. o mai bună colaborare între specialiștii de securitate și manageri;
3. eficiență ridicată în luarea deciziilor;
4. urmărirea evoluției incidentului și efectele măsurilor luate de specialiștii de securitate.

În ceea ce privește capabilitățile tehnice și operaționale ale CSIRT, menționez faptul că acestea se împart în trei categorii: *servicii proactive* (configurarea și mentenanța aplicațiilor gestionate în cadrul SIPOL și dezvoltarea instrumentelor de securitate, servicii de detecție a intruziunilor, precum și monitorizarea tehnologiilor din cadrul SIPOL), *servicii reactive* (alerte, atenționări, precum și managementul incidentelor, vulnerabilităților și artefactelor) și *servicii de management al calității securității* (analize de risc, planificarea „business continuity" și „disaster recovery", „training", informare și consultanță)[11].

Concluzii

Având în vedere progresul tehnologic la care societatea este martoră zi de zi, modalitatea în care se produce interacțiunea dintre om și tehnologie, modul în care tehnologia influențează instituțiile din domeniul ordinii și siguranței publice, evoluția securității cibernetice și a impactului acesteia asupra SISPOL, precum și riscurile și vulnerabilitățile în ceea ce privește informația electronică, considerăm oportună dezvoltarea la nivelul Poliției Române a propriului CSIRT. Prin crearea propriului CSIRT, Poliția Română va asigura compatibilitatea și interoperabilitatea SISPOL, va minimiza riscurile și vulnerabilitățile, va preveni incidentele majore și, nu în ultimul rând, își va proteja activele de valoare.

Echipa CSIRT, propusă a fi dezvoltată la nivelul structurii de poliție, va acumula date despre incidente, corelate cu potențialul atacurilor existente la un moment dat, al vulnerabilităților identificate, al prejudiciilor posibile și al măsurilor de securitate celor mai adecvate pentru contracarare. Pe cale de consecință, personalul CSIRT va asigura capabilitățile necesare analizării răspunsului la incidente și va contribui la îmbunătățirea măsurilor de securitate ca urmare a incidentelor care au afectat funcționarea SISPOL, în vederea coordonării și diseminării informațiilor, precum și alte activități legate de managementul incidentelor.

Pe lângă beneficiile menționate deja, echipa CSIRT va contribui la elaborarea de norme, instrumente și mecanisme pentru asigurarea rețelelor și sistemelor informatice de la nivelul Poliției Române, care să țină pasul cu evoluția amenințărilor cibernetice, în scopul garantării unui nivel ridicat de protecție al SISPOL. Scopul strategiei de securitate cibernetică propusă a fi dezvoltată la nivelul structurii de poliție este de a defini și de a menține un mediu virtual sigur la nivelul SISPOL, care să cuprindă obiectivele, principiile și direcțiile majore de acțiune pentru prevenirea și contracararea amenințărilor la adresa securității cibernetice, prin stabilirea și aplicarea unor profile de securitate relevante din punct de vedere al funcționării corecte a infrastructurii SISPOL.

Este de la sine înțeles că prevenirea săvârșirii unor infracțiuni prin mijloace de informare și monitorizare permanentă a securității SISPOL reprezintă cea mai bună cale de protecție a cetățenilor.

Note bibliografice:

[1] ***, *History of Innovation at the SEI*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, 2016, URL: https://www.sei.cmu.edu/about/history-of-innovation-at-the-sei, accesat la 04.02.2019.

[2] ***, *Ghid referitor la rolul structurilor de tip CERT și utilitatea CERT-urilor private*, Ghid realizat de către isec și provision în cadrul campaniei de conștientizare a riscurilor de securitate cibernetică derulată în România sub egida ECSM de către CERT-RO, URL: https://www.cert.ro/vezi/document/rolul-certuri lor-si-utilitatea-celor-private, accesat la 15.01.2019.

[3] *Ibidem*.

[4] *Hotărârea nr. 494 din 11.05.2011 privind înființarea Centrului Național de Răspuns la Incedente de Securitate Cibernetică - CERT-RO*, publicată în Monitorul Oficial, Partea I, nr. 388 din 02.06.2011.

[5] ***, „CERT-RO: Amenințările și vulnerabilitățile la adresa spațiului cibernetic național continuă să se diversifice. Numărul domeniilor „.ro" compromise în scădere", *CECCAR Business Magazine*, nr. 6, 21-27 februarie 2017, URL: http://www.ceccarbusinessmagazine.ro/cert-ro-amenintarile-si-vulnerabilitatile-la-adresa-spatiului-cibernetic-national-continua-sa-se-diversifice-numarul-domeniilor-ro-compromise-in-scadere-a1664, accesat la 15.01.2019.

[6] ***, *Raport privind evoluția amenințărilor cibernetice în 2017*, CERT-RO, 2018, URL: https://cert.ro/vezi/document/ra port-alerte-2017, accesat la 22.01.2019.

[7] „Cloud computing" reprezintă un „nou concept arhitectural de gestionare de la distanță a resurselor de procesare și stocare de date, iar tehnologia s-a dezvoltat atât de mult încât, acum, este suficient să-ți creezi un cont pe Amazon sau Yahoo pentru a putea dezvolta și lansa aplicații în Cloud" (Perhuru RAJ, *Cloud Enterprise Architecture*, CRC Press, 2013).
În literatura de specialitate sunt prezentate patru tipuri de Cloud: privat, public, de comunitate, hybrid. Astfel, termenul de „Cloud privat" descrie „o infrastructură IT, prevăzută pentru utilizarea exclusivă de către o singură organizație care cuprinde mai mulți consumatori. Infrastructura IT se află la sediul organizației sau gestionarea acesteia este externalizată la un terț („on-premises„ sau „off-premises"). Un „Cloud privat" poate fi comparat cu un centru de date convențional – diferența fiind că soluțiile tehnologice sunt puse în aplicare pentru a optimiza utilizarea resurselor disponibile și de a spori aceste resurse prin investiții mici, care sunt făcute într-un mod treptat în timp" (***, *Ghid Securitatea în Cloud*, Ghid realizat de Asociația Națională pentru Securitatea Sistemelor Informatice, București, 2012, p. 4, URL: https://www.cert.ro/vezi/document/securitatea-in-cloud, accesat la 18.01.2018).

[8] ***, *O abordare pas cu pas a modului de creare a unui CSIRT*, Produs final WP2006/5.1 (CERT-D1/D2), ENISA, URL: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-romanian/at_download/fullReport, accesat la 23.05.2019.

[9] Ransomware este o „specie de malware care blochează / restricționează total accesul utilizatorului la sistemul informatic (prin blocarea ecranului) sau la datele în format electronic (prin criptare), până când acesta plătește o răscumpărare către un terț" (****, Ghid de bune practici pentru securitate cibernetică,* p. 21, URL: https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf, accesat la 14.01.2019).
La nivelul Poliției Române, atacul Ransomware WannaCry nu a avut urmări notabile, numărul de stații infectate fiind unul foarte mic și criptarea acestora nu a avut loc datorită măsurilor luate.

[10] *Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică*, publicată în Monitorul Oficial al României, Partea I, nr. 296 din 23.05.2013.

[11] ***, *Ghid referitor la rolul structurilor de tip CERT și utilitatea CERT-urilor private*, Ghid realizat de către isec și provision în cadrul campaniei de conștientizare a riscurilor de securitate cibernetică derulată în Romania sub egida ECSM de către CERT-RO, p. 4.

Bibliografie:

1. ***, „CERT-RO: Amenințările și vulnerabilitățile la adresa spațiului cibernetic național continuă să se diversifice. Numărul domeniilor „.ro" compromise în scădere", *CECCAR Business Magazine*, nr. 6, 21-27 februarie 2017, URL: http://www.ceccarbusinessmagazine.ro/cert-ro-amenintarile-si-vulnerabilitatile-la-adresa-spatiului-cibernetic-national-continua-sa-se-diversifice-numarul-domeniilor-ro-compromise-in-scadere-a1664.

2. ***, *Ce reprezinta standardele Wi-Fi: IEEE 802.11a, 802.11b/g/n si 802.11ac ale unui router wireless*, URL: https://ihowto.tips/did-you-know/ce-reprezinta-standardele-wi-fi-ieee-802-11a-802-11b-g-n-si-802-11ac-ale-unui-router-wireless.html.

3. ***, *Ghid - Amenințări generice la adresa securității cibernetice*, Ghid realizat de către CERT.RO în cadrul campaniei de conștientizare a riscurilor de securitate cibernetică derulată în Romania sub egida ECSM de către CERT-RO, URL: https://cert.ro/vezi/document/amenintari-generice-securitate-cibernetica.

4. ***, *Ghid referitor la rolul structurilor de tip CERT și utilitatea CERT-urilor private*, Ghid realizat de către isec și provision în cadrul campaniei de conștientizare a riscurilor de securitate cibernetică derulată în România sub egida ECSM de către CERT-RO, URL: https://www.cert.ro/vezi/document/rolul-certurilor-si-utilitatea-celor-private.

5. ***, *Ghid de bune practici pentru securitate cibernetică*, URL: https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf.

6. ***, *Ghid Securitatea în Cloud*, Ghid realizat de Asociația Națională pentru Securitatea Sistemelor Informatice, București, 2012, URL: https://www.cert.ro/vezi/document/securitatea-in-cloud.

7. ***, *O abordare pas cu pas a modului de creare a unui CSIRT*, Produs final WP2006/5.1 (CERT-D1/D2), ENISA, URL: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-romanian/at_download/fullReport.

8. ***, *Raport privind evoluția amenințărilor cibernetice în 2017*, CERT-RO, 2018, URL: https://cert.ro/vezi/document/raport-alerte-2017.

9. ***, *History of Innovation at the SEI*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, 2016, URL: https://www.sei.cmu.edu/about/history-of-innovation-at-the-sei, accesat la 04.02.2019.

10. ***, *Îndrumar de planificare a securității cibernetice*, Q-East Software Smart Systems Management, Traducere în limba română după documentul „Cyber Security Planning Guide" întocmit de Federal Communications Commission din SUA, URL: https://cert.ro/vezi/document/q-east-indrumarul-de-planificare-a-securitatii-cibernetice.

11. *Comunicare Comună către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor, Strategia pentru securitate cibernetică a Uniunii Europene: un spațiu deschis, sigur și securizat*, Bruxelles, 07.02.2013.

12. *Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 06 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune*, publicată în Jurnalul Oficial al Uniunii Europene nr. L194/1 din 19.07.2016.

13. *Hotărârea nr. 494 din 11.05.2011 privind înființarea Centrului Național de Răspuns la Incedente de Securitate Cibernetică - CERT-RO*, publicată în Monitorul Oficial, Partea I, nr. 388 din 02.06.2011.

14. *Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică*, publicată în Monitorul Oficial al României, Partea I, nr. 296 din 23.05.2013.

15. *Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*, publicată în Monitorul Oficial al României, Partea I, nr. 21 din 12.01.2019.

16. *Regulamentul (UE) nr. 526/2013 al Parlamentului European și al Consiliului din 21 mai 2013 privind Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) și de abrogare a Regulamentului (CE) nr. 460/2004*, publicată în Jurnalul Oficial al Uniunii Europene nr. L165/41 din 18.06.2013.

17. *Regulamentul (UE) 2018/1726 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA) și de modificare a Regulamentului (CE) nr. 1987/2006 și a Deciziei 2007/533/JAI a Consiliului, precum și de*

abrogare a Regulamentului (UE) nr. 1077/2011, publicat în Jurnalul Oficial al Uniunii Europene nr. L295/99 din 21.11.2018.
18. ALEXANDRESCU, Grigore; VĂDUVA, Gheorghe, *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție*, Editura Universității Naționale de Apărare „Carol I”, București, 2006.
19. BALTAC, Vasile, *Tehnologiile informației - noțiuni de bază*, Editura Andreco Educaţional, București, 2011.
20. BUCUR, Ion I., *Tehnologii, structuri şi managementul reţelelor de calculatoare*, 2004.
21. BUTOI, Alexandru, *Contribuţii la disponibilitatea serviciilor și securitatea datelor în cloud computing*, Rezumat teză de doctorat, Facultatea de Științe Economice și Gestiunea Afacerilor, Universitatea Babeș-Bolyai, Cluj-Napoca, 2017, URL: http://193.231.20.119/doctorat/teza/fisier/3957.
22. COLLINS, Howard C.; HUGHES, Connor R. (eds), *Cyber Infrastructure Protection: Selected Issues and Analyses*, Nova Science Publishers, 2013.
23. HATHAWAY, Melissa E., *Best Practices in Computer Network Defense: Incident Detection and Response*, NATO Science for Peace and Security Series, D: Information and Communication Security - Vol. 35, IOS Press, 2014.
24. HOUSEHOLDER, Allen D.; WASSERMANN, Garret; MANION, Art; KINNG, Chris, *The CERT Guide to Coordinated Vulnerability Disclosure*, Special Report CMU/SEI-2017-SR-022, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, August 2017, URL: https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf.
25. KIRCH, Joel, *Virtual Machine Security Guideline - Version 1.0*, The Center for Internet Security, September 2007, URL: https://www.cisecurity.org/wp-content/uploads/2017/04/CIS_VM_Benchmark_v1.0.pdf.
26. KLANDER, Lars; RENEHAN Jr., Edward J., *Hacker Proof: The Ultimate Guide to Network Security*, Delmar Publishers, 2006.
27. MAGHERU, Ana-Maria, *Securitatea în rețelele wireless*, Lucrare de disertație, Facultatea de Electronică, Telecomunicații și Tehnologia Informației, Universitatea Politehnică, București, 2011, URL: http://stst.elia.pub.ro/news/RCI_2009_10/Teme_RCI_2011_12/MagheruAnaMaria/Securitate%20in%20retele%20wireless.pdf.
28. McCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George, *Securitatea reţelelor*, Editura Teora, București, 2002.
29. MELL, Peter; GRANCE, Timothy, *The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-145, September 2011, URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.
30. MIHAI, Ioan-Cosmin; PETRICĂ, Gabriel, *Securitatea informațiilor*, Ediția a II-a, Editura Sitech, Bucuresti, 2014.
31. MIHAI, Ioan-Cosmin; PETRICĂ, Gabriel; CIUCHI, Costel; GIUREA, Laurențiu, *Provocări și strategii de securitate cibernetică*, Editura Sitech, Bucuresti, 2015.
32. MIHAI, Ioan-Cosmin; CIUCHI, Costel; PETRICĂ, Gabriel-Marius, *Provocări actuale în domeniul securității cibernetice – impact și contribuția României în domeniu*, Studiul nr. 4, Studii de Strategie și Politici SPOS 2017, Institutul European din România, București, 2018, URL: http://www.ier.ro/sites/default/files/pdf/SPOS%202017_Studiul_4_FINAL.pdf.
33. MORARU, Sergiu, *Securitatea națională a Republicii Moldova în contextul democratizării societății: aspecte politico-informaționale*, Teza de doctorat, Chișinău, 2015, URL: http://www.cnaa.md/files/theses/2015/22863/moraru_sergiu_thesis.pdf.
34. NEAGARU, Daniel; COTEȚ, Dumitru, *Securitatea rețelelor: Metode de atac și protecție*, la Conferința Științifică „Spre Viitor”, Liceul Academiei de Științe a Moldovei, Chișinău, 2010, URL: http://www.pro-science.asm.md/docs/2010/uploaded_cresv10/securitatea_retelelor.docx.
35. OGÎGĂU-NEAMȚIU, Florin, *Cercetări privind securizarea informației în sistemele de cloud computing*, Rezumat teză de doctorat, Facultatea de Inginerie Electrică și știința Calculatoarelor, Universitatea Transilvania din Braşov, 2018, URL: https://www.unitbv.ro/documente/cercetare/doctorat-postdoctorat/sustinere-teza/2018/ogigau-neamtiu-florin/Rezumat_OGIGAU.pdf.
36. PATRICIU, Victor Valeriu; ENE-PIETROŞANU, Monica; BICA, Ion; PRIESCU, Justin, *Semnături electronice şi securitate informatică: aspecte criptografice, tehnice, juridice și de standardizare*, Editura Bic All, 2006.
37. POPA, Sorin Eugen, *Securitatea sistemelor informatice - note de curs și aplicații pentru studenții Facultății de Inginerie*, Universitatea din Bacău, 2007, URL: http://cadredidactice.ub.ro/sorinpopa/files/2011/10/Curs_Securit_Sist_Inf.pdf.
38. RAJ, Perhuru, *Cloud Enterprise Architecture*, CRC Press, 2013.
39. ROUSE, Margaret, *Wi-Fi Protected Access (WPA)*, May 2018, URL: https://searchmobilecomputing.techtarget.com/definition/Wi-Fi-Protected-Access.
40. TANENBAUM, Andrew S., *Rețelele de calculatoare*, Ediția a patra, Editura Byblos, Cluj-Napoca, 2003.
41. WEST-BROWN, Moira; STIKVOORT, Don; KOSSAKOWSKI, Klaus-Peter; KILLCRECE, Georgia; RUEFLE, Robin; ZAJICEK, Mark, *Handbook for Computer Security Incident Response Teams (CSIRTs)*, 2nd Edition, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, April 2003.

*Responsabilitatea privind conținutul articolelor publicate în **Colocviu strategic**, inclusiv a opiniilor exprimate, revine în totalitate autorilor, cu respectarea prevederilor Legii nr. 206 din 27 mai 2004 privind buna conduită în cercetarea științifică, dezvoltarea tehnologică și inovare și Legii nr. 8 din 14 martie 1996 privind dreptul de autor și drepturile conexe, cu modificările și completările ulterioare. Sunt autorizate orice reproduceri, fără perceperea taxelor aferente, cu condiția precizării exacte a numărului și anului de apariție ale publicației din care provin.*

Colocviu strategic
Redactor: CS II dr. Cristian BĂHNĂREANU
Pagină web: https://cssas.unap.ro/ro/cs.htm
e-ISSN 1842-8096, 1451/2019

Centrul de Studii Strategice de Apărare și Securitate
Adresă: șos. Panduri, nr. 68-72, sector 5, București
Telefon: 021.319.56.49, Fax: 021.319.57.80
E-mail: cssas@unap.ro, Site: https://cssas.unap.ro